IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA

UNITED STATES OF AMERICA,	)	
	)	Criminal No. 1:15-CR-048
v.	)	and
	)	Criminal No. 1:15-CR-051
	)	
BEAU BRANDON CROGHAN	)	**GOVERNMENT'S RESISTANCE**
and	)	**TO DEFENDANT'S MOTION**
STEVEN SHANE HORTON,	)	**TO SUPPRESS EVIDENCE**
	)	
Defendants.	)	

TABLE OF CONTENTS

Comes now the United States of America, by and through the United States Attorney for the Southern District of Iowa and the undersigned Assistant United States Attorney, Katherine A. McNamara, and hereby respectfully submits this resistance to the Defendant's motion to suppress evidence based upon an alleged violation of either the Federal Magistrates Act pursuant to Title 28, United States Code, Section 636, or Federal Rule of Criminal Procedure 41. In support of this resistance, the government states the following:

I. BACKGROUND

On February 20, 2015, the Federal Bureau of Investigation ("FBI") assumed administrative control of "Website A" which was a child pornography online bulletin board, the primary purpose of which was the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children.

The FBI operated Website A from February 20, 2015 until March 4, 2015, from a government-controlled computer server located in the Eastern District of Virginia. On February 20, 2015, the FBI obtained a search warrant from the Honorable Theresa Carroll Buchanan, United States Magistrate Judge for the Eastern District of Virginia, which permitted the FBI to utilize a "Network Investigative Technique" (the "NIT") during the time period that the FBI operated Website A (the "NIT search warrant"). Once a user logged into Website A, the NIT would cause the user's computer to reveal certain identifying information, including its Internet Protocol (IP) address.

In this particular case, among the IP addresses that were identified by the

NIT as accessing Website A were ones associated with the defendants, Beau Brandon Croghan and Steven Shane Horton (the "defendants"), which led law enforcement to each of the defendant's residences located in Southern District of Iowa. On July 17, 2015, and August 6, 2015, respectively, search warrants were obtained in the Southern District of Iowa by the FBI to search the residences of the defendants. The defendants were subsequently indicted and arrested on charges of access with intent to view child pornography involving a prepubescent minor, in violation of Title 18, United States Code, Section 2252(a)(5)(B).

The defendants have filed the instant motion seeking suppression of the information obtained by the NIT search warrant from the Eastern District of Virginia, which led to the identification and subsequent arrest of the defendants. The defendants file this motion to suppress on the claim that the Magistrate Judge in the Eastern District of Virginia did not have authority to issue the NIT search warrant under either the Federal Magistrates Act pursuant to Title 28, United States Code, Section 636, or Federal Rule of Criminal Procedure 41, and therefore, the NIT search warrant was issued void *ab initio*. For the reasons set forth below, the suppression motions should be denied in their entirety.

II. LAW

The Federal Magistrates Act established the jurisdiction and powers of United States Magistrate Judges. It provides that "each United States magistrate judge serving under it shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law" certain powers and duties, including

"all powers and duties conferred or imposed…by the Rules of Criminal Procedure for the United States District Courts." 28 U.S.C. § 636(a)(1).

Federal Rule of Criminal Procedure 41(b) addresses the authority of a magistrate judge to issue a warrant. It contains five (5) categories of authority that a magistrate has to issue a warrant at the request of a federal law enforcement officer or attorney for the government, which are: (1), a person or property located within the district; (2), person or property outside the district if the person or property is located within the district at the time the warranted is issued, but might move or be moved outside the district before the warrant is executed; (3), person or property within or outside the district in cases of domestic terrorism or international terrorism; (4), a tracking device which may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and (5), property outside the United States but that is within (A) a United States territory, possession or commonwealth; (B) the premises, regardless of owner, of a United States diplomatic or consular mission in a foreign state; or (C) a residence owned or leased by the United States and used by United States personnel assigned to a diplomatic or consular mission in a foreign state. Fed. R. Crim. Pr. 41(b)(1) – (5).

III. ARGUMENT

A. The NIT Search Warrant Complied with Rule 41.

Defendants argue that the NIT search warrant fails to satisfy Rule 41(b)(1) and (b)(2) because some of the computers that were searched by the NIT search warrant, including those of the defendants, were not located in the Eastern District

of Virginia, where the warrant was obtained, and that the server which hosted Website A, although located in the issuing district, was not where the search occurred. The defendants further argue that the NIT search warrant fails to satisfy Rule 41(b)(4) because "the installation of the NIT did not take place in the Eastern District of Virginia but in the district where the computer was physically located." *Id*. As a basis for this argument, the defendant relies on *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016), and *United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016).

In at least two other cases, however, it has been determined that the NIT search warrant was properly authorized by the magistrate judge pursuant to Federal Rule of Criminal Procedure 41(b)(4), which authorizes a magistrate judge to issue a warrant for a "tracking device" on person or property that is within the district, outside the district, or both. *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016) (accepting the tracking device theory that the NIT search warrant fits into 41(b)(1)(4), as anyone logging into Website A makes "a virtual trip" to Virginia); *United States v. Darby*, 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (finding that the magistrate had authority under 41(b)(4) to issue a warrant to deploy the NIT as a "tracking device").

In *Darby*, the district court found the tracking device subsection of Rule 41(b) to be "exactly analogous" to what the NIT search warrant authorized the FBI to do in this case. *Id*. Users of Website A essentially "digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government

about their location." 2016 WL 3189703 at *12. Furthermore, the district court in *Darby* reasoned that it was reasonable for the government to seek the NIT search warrant in the Eastern District of Virgnia, which was the district with the strongest ties to the case: "The government planned to run the website from a server located in the district [E.D. Va.]. No district in the country had a stronger connection to the proposed search than this district [E.D. Va.]. Additionally, nothing in Rule 41 categorically forbids magistrates from issuing warrants that authorize searches in other districts—most of its provisions do just that." *Id.* at *11.

Similarly, in *Matish*, the district court for the Eastern District of Virginia, (Newport News division), found that the magistrate was authorized to issue the NIT search warrant pursuant to Rule 41(b)(4) because the users of Website A made a "virtual trip" via the internet from the location of the user's computer to Virginia. 2016 WL 3545776 at *18. The court in *Matish* reasoned that because the NIT enabled the government to determine the location of the users of Website A, the NIT resembled a tracking device, and the NIT search warrant authorized the FBI to install a tracking device on each user's computer when that computer entered the Eastern District of Virginia (i.e., when the user logged into Website A). *Id.* The court distinguished the decision in *United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016), by stating: "…the installation did not occur on the government-controlled computer but on each individual computer that entered the Easter District of Virginia when the user logged into [Website A] via the Tor network. When that computer left Virginia—when the user logged out of [Website A]—the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location." *Id.*

The facts of these cases are no different here. The defendants logged onto Website A from computers located in the Southern District of Iowa, which triggered the NIT during the time period that the NIT tracking device was active, which gathered identifying information, including an IP address, for each of the defendant's computers. Relying on the holdings in *Darby* and *Matish*, *supra*, the NIT search warrant was property authorized by the magistrate judge and fully complied with Rule 41(b).

B. Even if the NIT Search Warrant Failed to Comply with Rule 41, the Violation was Merely Technical and Suppression is Not Warranted.

Defendants argue that the alleged jurisdictional violation of Rule 41 is constitutional, not technical, because the magistrate judge that signed the NIT search warrant had no authority to do so. Based on the above, it is the government's position that there was no violation of Rule 41 and that the magistrate judge in the Eastern District of Virginia had authority to issue the NIT search warrant. Even assuming, for the sake of argument, that the NIT search warrant was deficient due to a violation of Rule 41, suppression is neither required by law nor is suppression reasonable under the circumstances.

Although the purpose of Rule 41 is to carry out the mandate of the Fourth Amendments and its protections, **not all** Rule 41 violations render a search warrant invalid. Specifically, in the Eighth Circuit, the exclusionary rule is applied to violations of Rule 41 "only if a defendant is prejudiced or reckless disregard of proper procedure is evident." *United States v. Turner*, 781 F.3d 374, 387 (8th Cir. 2015) (citing *United States v. Bieri*, 21 F.3d 811, 816 (8th Cir. 1994)); *see also United*

States v. Freeman, 897 F.2d 346, 348-50 (8th Cir. 1990) (court refused to suppress evidence where technical violation of Rule 41 occurred).

Some district courts have found that there was a technical violation of Rule 41 when the magistrate judge in the Eastern District of Virginia issued the NIT search warrant – yet many of those courts have nonetheless found suppression to be **inappropriate**. *See United States v. Michaud*[1], No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (holding that the NIT warrant technically violated "the letter but not the spirit" of Rule 41(b) yet suppression was inappropriate); *United States v. Stamper*, No. 1:15-CR-109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016) (holding that the NIT warrant technically violated Rule 41(b) but "exclusion is not necessary because there has not been a showing of prejudice or an intentional and deliberate disregard of the Rule…"); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (finding issuance of NIT warrant violated Rule 41 but finding suppression to be inappropriate).

Accordingly, there have been no violations of Rule 41 in this case and suppression is certainly not a remedy even if there was a technical violation of the Rule.

C. Defendant Has Failed to Demonstrate Prejudice or Reckless Disregard by the Government.

The defendants argue for suppression of the evidence because the identification of the defendants and the subsequent search of their residences would

[1] In concluding that the NIT search warrant technically violated the "letter, but not the spirit" of Rule 41(b), the court in *Michaud* acknowledged that Rule 41 does not directly address the kind of situation that the NIT search warrant was authorized to investigate – "namely, where criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location." 2016 WL 337263 at *6.

not have occurred "but for" the alleged Rule 41 violation, and thus, the defendants suffered prejudice. In addition, the defendants argue that the government deliberately[2] disregarded the proper procedures of Rule 41.

Numerous district courts, however, even in cases where the court found that the NIT search warrant violated Rule 41, have found suppression to be unwarranted because the defendants have wholly failed to demonstrate that they suffered any prejudice or that the government deliberately disregarded proper procedures. *Michaud*, 2016 WL 337263 at *6-7 (W.D. Wash. Jan. 28, 2016) (finding that defendant suffered no prejudice nor did law enforcement act with deliberate disregard for proper procedures); *United States v. Stamper*, 1:15-CR-109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016) (same); *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (finding even if the warrant violated 41(b), suppression is inappropriate because the defendant showed neither prejudice nor that any violation was intentional or deliberate); *United States v. Epich*, No. 15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14. 2016) (acknowledging that violations of federal rules do not justify the exclusion of evidence that has been based on probable cause with advance judicial approval – "suppression of evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred"); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (finding that the government's actions were not prejudicial because they did not offend notions of fundamental fairness or due process).

[2] Note, as mentioned earlier in this brief, the standard in the Eighth Circuit for Rule 41 violations is "reckless" disregard, not "deliberate" as the defendants argue.

a. There is No Reasonable Expectation of Privacy in an Internet Protocol ("IP") Address

First, the information seized by the NIT did not lead to the defendants directly, but rather, provided law enforcement with an IP address from which the location of the defendants could be established. The NIT was minimally invasive in that it targeted only identifying information for the users of Website A and did not search the contents of the user's computer. *See Matish*, 2016 WL 3545776 at *22 (E.D. Va. 2016) (finding that the NIT was "programmed to collect very limited information […]" and "did not cross the line between collecting addressing information and gathering contents of any suspects computer").

Second, the defendant's IP address would ordinarily have been publicly available, had the defendants not utilized the Tor network to shield themselves from detection, and thus, the defendants have no reasonable expectation of privacy in that information. *United States v. Wheelock*, 772 F.3d 825, 828-30 (8th Cir. 2014) (holding that there is no expectation of privacy in the acquisition of subscriber information, including IP addresses, and no warrant was necessary); *United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (same).

In *Michaud*, the district court concluded that a Website A user "has no reasonable expectation of privacy in the most significant information gathered by deployment of the NIT, [his] assigned IP address," because even though "the IP addresses of users utilizing the Tor network may not be known to websites like Website A, using the Tor network does not strip users of all anonymity, because users accessing Website A must still send and receive information, including IP addresses, through another computer, such as an Internet Service Provider, at a

specific physical location." 2016 WL 337263 at *7 (W.D. Wash. Jan. 28, 2016); *see also Werdene*, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (holding that just because the defendant's IP address was "subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address…[Werdene] was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information"). The district court in *Matish* agreed with this reasoning, and went as far to conclude that a warrant would not have been needed at all in order to deploy the NIT technology to gather the identifying information of Website A users, given the lack of privacy interest in an IP address, and compared the information gathered by the NIT to the information gathered by a pen register. 2016 WL 3545776 at *22-24.

The defendants have no objectively reasonable expectation of privacy in their IP addresses and thus, have suffered no prejudice from this information being revealed to law enforcement through the NIT search warrant. Once each defendant's location was verified from the IP address, a separate search warrant in the Southern District of Iowa was obtained to subsequently search their residences, further covering the constitutional basis for the government's search and seizure in this case.

b. There was no Reckless Disregard of Procedure by the Government

Defendants argue that the alleged violation by the government was deliberate because the Department of Justice has been trying to amend Rule 41(b) to allow explicitly this type of warrant. Therefore, defendant argues that the special

agents with the FBI that obtained the NIT search warrant allegedly knew that the NIT search warrant was "not authorized" by Rule 41(b).

The defendant in *Darby* made a similar argument regarding the Department of Justice's proposed amendment to Rule 41(b) with respect to electronic storage media, and the court's response was, in basic terms, that this argument is "absurd": "Defendant seeks to attribute to the FBI agents that sought the warrant the legal expertise of the DOJ lawyers, which is absurd. As discussed above, it was quite logical for the FBI to seek this warrant in the Eastern District of Virginia. Even if this Court is incorrect in holding that there was no violation of Rule 41(b), there is a credible argument that the current rule [41] allowed this warrant." 2016 WL 3189703 at *12 (E.D. Va. June 3, 2016). The court went on to say, "If they [the FBI] were so inclined to undermine individual rights, they might have foregone seeking the warrant in the first place" and "any violation of Rule 41(b) was unintentional." *Id*.

The district court in *Michaud* also rejected the defendant's argument that there was deliberate disregard by the government because the government has previously argued that Rule 41(b) should be amended to account for changes in technology, "given that reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in unchartered territory." 2016 WL 337263 at *15 (W.D. Wash. Jan. 28, 2016).

The defendant cannot show that any variance from the text of Rule 41(b) warrants suppression as an intentional and deliberate disregard of the rule, let alone "reckless disregard" for proper procedure, which is what the Eighth Circuit requires. *Turner*, 781 F.3d at 387 (8th Cir. 2015). The proposed amendment to

Rule 41(b) and the Department of Justice's support of said amendment shows that the government recognizes the need for clarification of the Rule – given the evolution of technology – but it certainly does not show that Rule 41 is a complete bar to the approach taken by the government when it obtained the NIT search warrant[3]. The NIT search warrant that was obtained was the product of a large scale investigation by FBI agents who, rather than failing to obtain a warrant, deliberately sought to satisfy Rule 41 by seeking a warrant in the district with the greatest known connection to the criminal activity – the Eastern District of Virginia. The FBI reasonably concluded that the magistrate could issue the NIT search warrant when the property (the server) was located in the Eastern District of Virginia and the NIT would travel outside of the that district only after individuals, who had already taken steps to shield their location by using the Tor network, accessed the server and requested the content of Website A. In the NIT search warrant affidavit, the FBI was candid about the fact that the NIT would be deployed into computers that accessed Website A, wherever they were located.

No evidence exists to support the contention of the defendants that the agents who obtained the NIT search warrant "recklessly disregarded" the proper procedures under Rule 41, as the Eighth Circuit requires.

[3] "The pending [Rule 41] amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes. That is, there is nothing unreasonable about the scope of the warrant itself. The FBI should be applauded for its actions in this case." *Darby*, No. 2:16-CR-36, 2016 WL 3189703 at *13 (E.D. Va. June 3, 2016).

D. The Good Faith Exception Applies.

For all of the reasons above, the NIT search warrant did not contravene the requirements of the Fourth Amendment. Even if the NIT search warrant is found to be deficient, the search of computers outside of the territorial limits of the Eastern District of Virginia was lawful under the good faith exception to the Fourth Amendment's exclusionary rule as recognized in *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). The Supreme Court has recognized that exclusion of evidence is a "last resort" not a "first impulse." *Herring v. United States*, 555 U.S. 135, 129 S.Ct. 695, 700 (2009).

Evidence obtained pursuant to an invalidated search warrant need not be excluded if the executing officers acted in objectively reasonable reliance on the issuing court's determination of probable cause and technical sufficiency. *Leon*, 468 U.S. at 922-923; and *United States v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007). Absent proof that the issuing judge was not neutral, officers were dishonest or reckless in preparing the affidavit, or could not have harbored an objectively reasonable belief in the existence of probable cause, the good faith exception should be applied. *Leon*, 468 U.S. at 926. The Eighth Circuit has made clear that the government must fail a high threshold of unreasonableness before the court will refuse to apply the good faith exception. *See*, *Proell*, at 432.

Here, the NIT search warrant affidavit did not contain false statements of facts[4] that were material to the issue of probable cause, nor is there any evidence of recklessness by the government agents in the preparation of the affidavit. The NIT

[4] This district court in *Werdene* acknowledged that "this is not a case where the agents hid the ball from the magistrate or misrepresented how the search would be conducted." No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016)

search warrant made clear how the search would be conducted and where it would be done. Further, there is absolutely no evidence or even a suggestion that the magistrate judge in that district was anything but detached and neutral when she authorized the NIT search warrant. Thus, once the magistrate judge signed the NIT search warrant, the agents' reliance on the magistrate's authority was objectively reasonable. The good faith exception to the exclusionary rule should be applied in this case – should the court find the NIT search warrant to be invalid.

In addition, there is a great societal cost if the court grants suppression in this case (which the court in *Levin*, a case upon which the defendants so heavily rely in their motion, failed to analyze). If suppression is granted in this case the societal costs are substantial, given that suppression "almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence…and its bottom-line effect…is to suppress the truth and set the criminal loose in the community without punishment." *Davis v. United States*, 564 U.S. 229, 237, 131 S.Ct. 2419, 2427 (2011). As stated by Senior District Court Judge Henry Coke Morgan Jr. in *Matish*, "The Government's efforts to contain child pornographers, terrorists and the like cannot remain frozen in time; it must be allowed to utilize its own advanced technology to keep pace with our world's ever-advancing technology and novel criminal methods." No. 4:16-CR-16, 2016 WL 3545776 at *44 (E.D. Va. June 1, 2016). Suppression in these cases involving the NIT search warrant would only serve to exact "a heavy toll on both the judicial system and society at large." *Davis*, 564 U.S. at 237 (2011).

IV. CONCLUSION

WHEREFORE, based upon the aforementioned, the government respectfully requests that this court deny the motion to suppress in its entirety. The government further requests that, if a hearing on this matter is ordered, the court consolidate the cases for the purposes of said hearing, given that the arguments for suppression in each motion appear to be identical.

Respectfully Submitted,

Kevin E. VanderSchel
United States Attorney

By: */s/ Katherine A. McNamara*
Katherine A. McNamara
Assistant United States Attorney
P.O. Box 1887
Council Bluffs, Iowa 51502
Tel: 712-256-5009
Fax: 712-256-5112
Email: Katherine.McNamara@usdoj.gov

CERTIFICATE OF SERVICE
I hereby certify that on July 27, 2016, I electronically filed the foregoing with the Clerk of Court using the CM ECF system. I hereby certify that a copy of this document was served on the parties or attorneys of record by:
____U.S. Mail _____ Fax _____Hand Delivery
_X___ECF/Electronic filing ____Other means
UNITED STATES ATTORNEY
By*: /s/KAM*, AUSA___